**Prac4A: Index Key exchange using Diffie - Hellman**

**! Write Small theory !**

**! Write Algo !**

**! Write Solved Numerical !**

**Code:**

**— Java —**

package com.mycompany.tycs.rehmah;

import java.util.\*;

public class Prac4 {

public static void main(String[] args){

Scanner sc = new Scanner(System.in);

System.out.println("Enter 2 numbers P an G, agreed on by both users:");

int p = sc.nextInt();

int g = sc.nextInt();

System.out.println("Enter Alice's secret key: ");

int a = sc.nextInt();

System.out.println("Enter Bob's secret key: ");

int b = sc.nextInt();

int x = (int)Math.pow(g, a)%p;

int y = (int)Math.pow(g, b)%p;

System.out.println("X="+x);

System.out.println("Y="+y);

int Ka = (int)Math.pow(y, a)%p;

int Kb = (int)Math.pow(x, b)%p;

System.out.println("Secret key for Alice is "+Ka);

System.out.println("Secret key for Bob is "+Kb);

}

}

**Output:**

Enter 2 numbers P an G, agreed on by both users:

23

9

Enter Alice's secret key:

3

Enter Bob's secret key:

4

X=16

Y=6

Secret key for Alice is 9

Secret key for Bob is 9

**Code:**

**— Python —**

p = int(input("Enter Prime number P: "))

g = int(input("Enter primitive root number G: "))

a = int(input("Enter Alice's secret key: "))

b = int(input("Enter Bob's secret key: "))

x = int(pow(g, a ,p))

y = int(pow(g, b, p))

print("X=", x)

print("Y=", y)

k1 = int(pow(y, a, p))

k2 = int(pow(x, b, p))

print("Secret key for Alice: ", k1)

print("Secret key for Bob: ", k2)

**Output:**

Enter Prime number P: 23

Enter primitive root number G: 9

Enter Alice's secret key: 3

Enter Bob's secret key: 4

X= 16

Y= 6

Secret key for Alice: 9

Secret key for Bob: 9